



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 14 January 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- Reuters reports bitterly cold weather headed for the Northeast has forced some natural gas distributors to halt deliveries to businesses to ensure there is enough gas to meet home heating demand. (See item [3](#))
- Microsoft has released "Security Bulletin MS04-003: Buffer Overrun In MDAC Function Could Allow Code Execution" (Important) and applicable tools, security update, and workarounds are available on the Microsoft Website. (See item [26](#))
- Microsoft has released "Security Bulletin MS04-001: Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Can Allow Remote Code Execution" (Critical) and applicable tools and workarounds are available on the Microsoft Website. (See item [27](#))
- CNN reports on the second anniversary of the September 11 attacks, investigators found persistent and severe security deficiencies throughout the National Mall. (See item [32](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

January 13, Reuters — **OPEC calls for halt to oil price surge. OPEC's president on Tuesday, January 13, appealed for high-flying oil markets to stabilize as signals grew that sustained price strength will make it hard for the cartel to enact an expected supply cut next month.** U.S. crude has blazed to 10-month highs, topping \$35 a barrel for the first time since the Iraq war, on fears that freezing U.S. weather will strain crude oil stocks already at their lowest level since 1975. "We are calling on all parties involved in the oil markets to take an initiative to keep prices stable in the position that represents producers and consumers," said OPEC President Purnomo Yusgiantoro, Indonesia's oil minister. **OPEC ministers said last month that they expected to cut supply again at a February 10 meeting, fearing a surplus in the second quarter as demand declines after the northern winter. Ministers on Tuesday signaled that a February cut is now not a foregone conclusion.** Rapid economic growth in China has pumped up fuel demand, while sabotage at Iraqi oil facilities has delayed its post-war production recovery.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12420-2004Jan 13.html>

2. *January 13, Associated Press* — **Missing gauge with nuclear material recovered. Baltimore, MD, authorities say a stolen moisture density gauge containing nuclear material has been recovered. The gauge remained locked while it was missing, and no radioactive material was able to escape.** It's not a hazard to the public as long as it's locked. The gauge was reported missing on Friday, January 9. Baltimore County police have identified two suspects in the theft. Police got a tip Saturday, January 10, that led to the gauge being recovered at the end of Smallwood Street, near the Baltimore city line and not far from Halethorpe, where it was reported stolen.

Source: <http://www.insidebaltimore.com/news/local/04-01-13-nuc.shtml>

3. *January 13, Reuters* — **Cold pinches northeast U.S. gas supplies. Bitterly cold weather headed for the Northeast later this week has forced some natural gas distributors to halt deliveries to some businesses for the second time in a week to ensure there is enough gas to meet home heating demand. The looming deep freeze is expected to strain utilities' capacity to deliver gas, forcing cuts to some commercial and industrial firms that buy gas at a discount under so-called interruptible contracts.** Such customers know their supply may be curtailed on short notice during peak demand periods. The scramble for supplies doubled gas prices in New York City on Tuesday, January 13, with next-day deliveries fetching \$16.35 per million British thermal units, up from \$7.73 on Monday, January 12. "We have notified 77 of our customers who have interruptible contracts that their service will be interrupted at 10 a.m. tomorrow [January 14] in anticipation of the unusually cold weather," said utility PSE&G spokesperson Karen Johnson. A company spokesperson for KeySpan Corp. said all New England interruptible customers have been shut off since last week.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A13471-2004Jan 13.html>

[[Return to top](#)]

Chemical Sector

4. *January 13, NewsNet 5 (Ohio)* — **Homes evacuated after large Ohio plant fire breaks out.** A large structural fire at a chemical plant in Avon, OH, caused two area homes to be evacuated this morning, January 13, when a fire broke out. **A fire broke out Chemtron at about 10:15**

Tuesday morning. It is now under control. There were also a few explosions because of propane tanks, but the fire is in a non-regulated, non-hazardous portion of the plant. Chemtron is a waste disposal company that responds to emergency chemical spills. Officials said the fire is not similar to a recent magnesium fire at Garfield Alloy. The plant, located on Schneider Court Road, was fully engulfed. North Ridgeville, Westlake, Avon Lake and Avon fire departments are at the scene. Large plumes of smoke could be seen from miles away. There's no word yet on a cause. No one was injured.

Source: <http://cms.firehouse.com/content/article/article.jsp?id=sectionId=46&id=24420>

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *January 13, Associated Press* — **Air Force wants to put fighters on Guam. The Air Force wants to begin basing fighter jets and other strike and support planes on Guam, the Pacific island that is in ready striking distance of the Korean peninsula, the Air Force's top officer in the region said Tuesday, January 13. "It's an active proposal," said General William J. Begert, commander of U.S. Pacific Air Forces. "The ability to project force from Guam is very valuable to us," Begert added.** Aircraft and other U.S. offensive forces that had been based on Guam during the Cold War were withdrawn during the 1990s defense budget cuts and drawdown of U.S. military capabilities worldwide. A few years ago the Air Force began building up the infrastructure on Andersen Air Force Base, the main air base on Guam, including stockpiling large amounts of munitions. Begert pointed out that Guam is about 1,500 miles from the Korean peninsula and a similar distance from the Taiwan Straits, which is a potential flashpoint for conflict with communist China.

Source: <http://www.newsday.com/news/politics/wire/sns-ap-us-forces-pacific.0,1814807.story?coll=sns-ap-politics-headlines>

6. *January 13, Associated Press* — **Air Force Academy grounds 45 aircraft. The military grounded 45 aircraft at the Air Force Academy for safety reasons Tuesday, January 13, after discrepancies were discovered in a contractor's maintenance records.** Academy officials said they will investigate the discrepancies and keep the aircraft on the ground until "confidence is restored in the safety of the maintenance program and permanent fixes are in place." Safety concerns were heightened following the January 2 engine failure of a twin-engine UV-18 Twin Otter aircraft. The aircraft was en route to Florida to pick up cadets participating in a parachuting competition when it was forced to land at Tinker Air Force Base, OK. **The grounding affects such aircraft as UV-18s, Cessna 150s, gliders and motorized gliders.**

Source: http://abcnews.go.com/wire/US/ap20040113_1046.html

[\[Return to top\]](#)

Banking and Finance Sector

Nothing to report.

[\[Return to top\]](#)

Transportation Sector

7. *January 13, The Trucker* — **Road condition hotline moving across country.** More states have begun using the 511 service approved in 2000 for traffic reports. **The 511 hotline, was designed as a source of information about accidents, delays, weather-related road conditions and road construction. The abbreviated dialing code for travel information services has gained some speed lately as Oregon became the 18th state to use the 511 number.** Fifteen states have 511 in use for all roads, with Kansas set to join soon. Other locations using the system are: San Francisco, Cincinnati, South Florida, Orlando, FL, and the I-81 Corridor in Virginia, according to Rich Taylor, director, information programs at Intelligent Transportation Society of America (ITS). The U.S. Department of Transportation was granted its petition to establish the national three digit dialing code in July 2000 by the Federal Communications Commission, which then assigned 511 as the abbreviated dialing code for travel information services, according to a summary of the FCC's report and order. Source: http://www.thetrucker.com/stories/01_04/0113_hotline.html
8. *January 13, Army News Service* — **Soldiers increasingly trying to carry prohibited items on airliners.** Increasingly soldiers are attempting to carry prohibited items on commercial airliners either going to or returning from an overseas assignments, officials said. This act could be a career ender for soldiers under the Uniformed Code of Military Justice, said Chet Spangler, Air Traffic Control staff specialist, Headquarters, U.S. Army Aeronautical Services Agency. **"Recently, the Transportation Security Administration confiscated various items to include five pounds of fireworks, brass knuckles with a four-inch knife blade, a loaded BB pistol and a nine-millimeter pistol during airport security checks," Spangler said.** According to the United States Code of Federal Regulations, a person who attempts to carry prohibited items on an airplane is subject to a \$10,000 civil penalty. The junior soldier who was detained for checking a landmine in his baggage was not charged with a criminal offense, but could face civil penalties, according to an article by the Denver bureau of the Associated Press. **Commanders are strongly encouraged to thoroughly brief Soldiers on which items are prohibited when traveling on civilian air carries to prevent future violations,** officials said. Source: http://www4.army.mil/ocpa/read.php?story_id_key=5583
9. *January 13, Australian Broadcasting Corporation* — **Uzbek plane crash leaves 37 dead.** A passenger plane has crashed near the Uzbek capital of Tashkent killing 37 people, the ITAR-TASS news agency reported. ITAR-TASS described the plane as an An-24 but an Uzbek Emergencies Ministry official contacted by AFP said it was a smaller, Yak-40 passenger jet. **Initial reports said the plane was flying from the southern town of Termez on the border with Afghanistan to the Uzbek capital. One report added to the overall confusion concerning the accident, saying the plane crashed upon takeoff.** Reports said the plane belonged to a local Uzbek airline and that Uzbek President Islam Karimov went to the site of the crash near the capital of the Central Asian country, ITAR-TASS reported. Ground contact with the jet was lost at around 7:45 pm local time, Interfax said. The Yak-40 was first built in 1966 and was designed for short-haul flights and is today widely used throughout the former Soviet Union. **Analysts say it has one of the best safety records of any Soviet-built plane, although financial difficulties of many airlines in post-Soviet countries has increased reliance on aging jets.** Meanwhile, information about the latest accident was

limited, with several conflicting reports. Uzbekistan is seen as one of the most authoritarian regimes in Central Asia, with tight control of the press and limited access to public officials. Source: <http://www.abc.net.au/news/newsitems/s1025009.htm>

10. *January 13, Eupolitix.com* — **Brussels calls for airline transparency.** Brussels is to consider how holiday makers can gain better information about the airlines which fly them on package holidays, transport Commissioner Loyola de Palacio said on Monday. **Speaking at a EU parliament debate in Strasbourg, the Commissioner said that while companies provide information about accommodation, food and activities, there is "no information on the airline company which is providing the transport...It is important that we think hard about the way tour operators operate, especially the information that is provided to passengers about the airline."** The Commissioner added, "I have asked the services of the Commission to look into this matter with priority because it is essential." Palacio told MEPs that the recent crash of the Egyptian airlines highlighted the importance of improving airline safety. The charter airline was banned from entering Swiss airspace but inspected and found safe by French authorities.
Source: <http://www.eupolitix.com/EN/News/200401/e7b594ea-c372-4ebe-b334-f3f7dbf2ad8c.htm?WBCMODE=PresentationUnpublished>
11. *January 13, Agence France-Presse* — **British Airways chief says airline will accept armed sky marshals.** The chief executive of British Airways said Tuesday his airline would accept the presence of armed sky marshals on its flights, but only under strict conditions. **The comments by BA chief executive Rod Eddington in an article published in the Financial Times, follows earlier reports that the British flag carrier would rather cancel flights than be forced to accept guns on its planes.** Eddington also acknowledged that security alerts which caused a series of BA flights to the United States and the Middle East to be cancelled or delayed just after Christmas were necessary in the era of global terrorism. "However, I accept that in the current climate an armed police officer, correctly deployed, on board a particular flight might have a place in aviation security," Eddington wrote. **"Our position at British Airways is that if, indeed, security on a particular flight could be enhanced by the onboard presence of an armed police officer, we would be happy to accept that fact.** "Equally, we maintain that if we have any cause for concern regarding the safety or security of a particular flight, we would simply not operate that service. We demonstrated that with the recent cancellations," he said. However, any deal to allow guns onto BA flights would have to meet "exacting criteria", Eddington added, saying he could not give any details for security reasons.
Source: http://www.usatoday.com/tech/news/2004-01-13-ba-marshals_x.htm
12. *January 13, WUSA 9 News* — **Tanker truck explodes in accident on I-95 in Maryland.** At least two people were killed Tuesday afternoon in a collision and fire along Interstate 95, a Howard County (MD) fire department spokesman said. **The accident occurred shortly before 3 p.m. in the northbound lane of the highway, just below an overpass carrying the southbound lane of Interstate 895, said William Mould, the fire department spokesman. The accident involved two automobiles and two tractor trailers -- one a tanker truck and one a box-type truck. It sparked a four-alarm fire and there were hazardous materials involved,** he said. He did not know what cargo the trucks were carrying. The fire burned for about an hour. Firefighters from Howard County, Baltimore County, and

Baltimore–Washington International Airport responded to the scene. Firefighters sprayed foam to contain the flames. "There was fire everywhere," said Chuck Gischlar, an SHA spokesman. "It was down in the woods, on other vehicles. It was terrible there." From an aerial image, Gischlar said he saw the tanker truck, another tractor trailer and at least one passenger vehicle in the accident. Traffic was backed up in both directions on I–95, and authorities were working to establish a detour. The scene is near Baltimore–Washington International Airport, and people there could see the smoke.

Source: http://www.wusatv9.com/news/news_article.aspx?storyid=26024

[[Return to top](#)]

Postal and Shipping Sector

13. *January 13, Associated Press* — **Interpol widens network after parcel bombs.** Interpol said on Tuesday that it will broaden access to its new global communications network so information can be shared on potential security threats and terrorist attacks. **Interpol's decision to grant some international institutions access to its state-of-the-art "I–24/7" network follows a spate of letter bombs sent to European officials.** The move will enable security officials from other institutions, including the European Union, to instantly share information on security threats, Interpol said in a statement. **International organizations will have the chance to post and view data on suspicious parcels.** Officials from the international police agency decided to broaden access to the heavily encrypted system after talks with Italian officials. Italy is leading an investigation into a shadowy anarchist group suspected in a string of booby–trapped letters sent to European Union authorities in five countries. All the letters bore Bologna, Italy postmarks and were mailed around December 22.

Source: <http://timesofindia.indiatimes.com/articleshow/420837.cms>

14. *January 09, Kansas City Business Journal* — **Yellow Roadway plans to add shipping terminals.** Yellow Roadway Corp. CEO Bill Zollars said Friday that the company is preparing to expand in 2004 by opening new shipping terminals in U.S. towns where neither Yellow Transportation nor Roadway Express could previously afford to have them. Combined, the two companies haul sufficient loads to many such towns to justify the cost of opening new terminals, he said. **At the company's 745 terminals, crews move shipments from local trucks that deliver and pick up goods from businesses to longer–haul trucks that operate between terminals. United Parcel Service and FedEx are muscling into the market, blurring the distinction between the package delivery industry and the less–than–truckload business.**

Source: <http://kansascity.bizjournals.com/kansascity/stories/2004/01/05/daily45.html>

[[Return to top](#)]

Agriculture Sector

15. *January 13, Associated Press* — **Disease hits Vidalia onions. Researchers are scrambling to identify a mystery disease that has emerged for the first time as a threat to Georgia's \$75 million crop of Vidalia sweet onions. Tests are being conducted on lesions that have**

started appearing on the leaves of onion plants in seed beds. Scientists are trying to find out whether they have a unique cause or are related to tomato spotted wilt virus, which has plagued Georgia peanuts and tobacco, or iris yellow spot virus, which has damaged onion crops in South America and the northwestern United States. "This is the first year it's come to our attention," said Reid Torrance, a University of Georgia extension coordinator in Tattnall County, the state's largest Vidalia-producing county. The disease does not appear to be any of the typical bacterial or fungal diseases that attack onions, Torrance said. Georgia Agriculture Commissioner Tommy Irvin said the disease has created a "serious situation" and his department would do all it could to prevent its spread.

Source: http://story.news.yahoo.com/news?tmpl=story&u=/ap/20040113/ap_on_bi_ge/farm_scene_1

16. *January 13, China View* — **Bird flu hits South Korean farm again. Bird flu has again hit a poultry farm in southeastern South Korea, killing 9,000 chickens, the Korean Ministry of Agriculture and Forestry confirmed Tuesday. It is the nation's first confirmed outbreak in nine days, increasing the number of confirmed cases to 16 since the first outbreak on December 15.** Authorities started an investigation last Saturday after a farmer in Yangsan reported that chickens at the farm died of unknown causes. "The suspected case proved positive for the bird flu virus," said Kim Chang-seob, chief of the animal health division at the ministry. Kim also said that the government imposed a ban on chicken imports from Japan on Monday after it was reported that about 6,000 chickens died from bird flu at a farm in Japan's Yamaguchi prefecture. The H5N1 virus, which raged through South Korea last month, appeared to have been brought under control at the beginning of the new year after about 1.6 million chickens and ducks were culled as an effort to prevent the spread of the disease.

Source: http://news.xinhuanet.com/english/2004-01/13/content_1273981.htm

17. *January 13, Agricultural Research Service* — **Grain sorter sees fungal poisons. An Agricultural Research Service (ARS) engineer, through the use of near-infrared spectroscopy, has transformed a standard grain sorter into a fast and highly effective detector of the mycotoxins that cost the corn industry millions of dollars each year.** Mycotoxins are natural compounds produced by some fungi. Occurring on corn, cottonseed, wheat, and other crops, they can cause serious illness in animals and livestock and are considered carcinogenic to humans. Thomas C. Pearson adapted a commercially available grain sorter to detect two types of mycotoxins that commonly infest corn: aflatoxin, which is produced by some strains of the fungus *Aspergillus flavus*, and fumonisin, produced by fungi of the genus *Fusarium*. Pearson found that two bands of infrared light are needed to detect almost all kernels of corn contaminated with aflatoxin and fumonisin. He equipped a grain sorter with a pair of filters corresponding with these wavelengths. **With just one pass through the sorting machine, 80 percent or more of the aflatoxin and fumonisin in commercially grown and harvested corn can be detected and removed.** The sorter erroneously rejects less than five percent of uncontaminated corn, compared to error rates of 10 percent or higher for other sorting machines.

Source: <http://www.ars.usda.gov/is/pr/2004/040113.htm>

18. *January 13, Reuters* — **U.S. sees drop in beef exports. The loss of export markets for U.S. beef following the discovery last month of the first case of mad cow disease in the U.S. will significantly lower cattle prices in 2004, the U.S. Department of Agriculture (USDA) said**

Monday. U.S. cattle prices were forecast in the range of \$72 to \$78 per hundredweight, down from a government estimate last month of \$84 to \$91 for 100 pounds of beef this year. **In its monthly crop report, the USDA said U.S. beef exports would fall by 90 percent this year after virtually all foreign countries, except Canada, banned U.S. beef.** A Holstein cow slaughtered on December 9 in Washington state was found to have mad cow disease. Since the December 23 announcement of the Washington state case, investigators have found the animal was born in Canada, and U.S. officials have said they are hopeful this will be an isolated case. **USDA noted in its crop–production report that the impact of the case on meat production is "expected to be minimal" with domestic demand for beef remaining "firm."**

Source: <http://www.iht.com/articles/124685.htm>

[\[Return to top\]](#)

Food Sector

19. *January 13, Dow Jones Newswires* — **Japan rejects Canada's request to end beef import ban.** Japan's Agriculture, Forestry, and Fisheries Minister Yoshiyuki Kamei has rejected Canada's request to lift Japan's import ban on Canadian beef. Kamei conveyed the decision on Tuesday after Canadian Agriculture Minister Bob Speller briefed him on measures the Canadian government took to ensure the safety of the country's beef, ministry officials said. Speller arrived in Tokyo earlier Tuesday on a mission aimed at persuading Japan to remove the import ban it imposed soon after Canada announced the discovery of its first case of mad cow disease last May. It was confirmed last week that a U.S. cow found infected with the brain–wasting disease last December was born in Canada. **Japan has called on Canada to take thorough steps to ensure the safety of Canadian beef before it can lift the import ban. Kamei has said he wants Canada "to test all cattle as the Japanese government does, or take measures that would have the same effect."**

Source: http://www.agprofessional.com/show_story.php?id=23063

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

20. *January 13, Tufts Center for the Study of Drug Development* — **FDA will be pressed to do more with less. Pressure on the U.S. Food and Drug Administration (FDA) to maintain staff expertise will grow during 2004 as experienced agency staff retire or change jobs, and fewer new product applications limit funds available for new hires, according to the Tufts Center for the Study of Drug Development.** Adding to the FDA's burden is an expanded mission to implement counter–bioterrorism activities, review increasingly complex new product applications, and expand post–market safety vigilance, the Tufts Center reported in its recently released Outlook 2004 report on drug and biotech development trends. "FDA

personnel and resources will be under growing stress to carry out its primary mission to ensure the marketing of safe and effective medicines in the U.S.," said Tufts Center Director Kenneth I Kaitin. He added, "Drug developers are now expected to include more extensive data sets when submitting new drug applications, and the FDA is faced with the formidable challenge of evaluating this information efficiently without slowing down the approval process."

Source: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040113005028&newsLang=en

21. *January 13, Associated Press* — **Montana State University receives contract for drug study. Montana State University (MSU) has won a \$10.5 million federal contract to research new drugs to fight diseases such as anthrax that could be used by terrorists. The goal is to develop a pill that people could take to strengthen their natural immune defenses,** said Mark Jutila, the MSU immunology professor in charge of the research. In addition to doing basic science, MSU scientists will work a Bozeman, MT, company that has been developing drugs to treat inflammatory and infectious diseases. The company and MSU will screen up to 200,000 compounds to find the most effective drug. Lethal organisms such as anthrax, smallpox, and plague will not be tested at the MSU labs, Jutila said. Instead, researchers will investigate how to boost the body's defenses by focusing on one cell in the intestines, called the gamma-delta T-cell. He plans to study the gamma-delta T-cell "receptors," which recognize infections and kick-start the body's defenses. If the T-cells could be made stronger, faster, or more numerous, they would ward off a variety of infections.

Source: <http://www.billingsgazette.com/index.php?id=1&display=rednews/2004/01/13/build/state/50-msudrugs.inc>

22. *January 13, Reuters* — **Travelers urged to get vaccinated for diphtheria. A Pennsylvania man who died of diphtheria last year likely contracted the disease in Haiti, according to U.S. health officials, who urged American travelers on Thursday to stay vaccinated against the disease.** Diphtheria, which typically causes soreness in the throat and difficulty breathing but in serious cases paralysis, coma, and heart failure, was common in the U.S. until the advent of mass vaccination programs in the 1940s. The disease is still active in more than 80 countries, mostly in the developing world, where it kills up to 20 percent of its victims. The 63-year-old Pennsylvania man died of cardiac complications about three weeks after first complaining of a sore throat during a volunteer mission to Haiti in October, 2003, according to an investigation by the Centers for Disease Control and Prevention (CDC). U.S. lab tests eventually confirmed the presence of diphtheria-causing bacteria in the man, the CDC report said. **The U.S. recommends that all travelers, regardless of age or destination, receive a primary series of three or more doses of the diphtheria vaccine, including a booster within the preceding 10 years before going abroad.** Most Americans are vaccinated against tetanus and diphtheria as children. Protection against the diseases, however, drops to less than 50 percent by the age of 20.

Source: http://www.abcnews.go.com/wire/Travel/businesstraveler/reuters20040108_436.html

23. *January 13, HealthDayNews* — **Blood donations slow.** January is typically a tough month for blood centers looking to collect donations. Some of the reasons are seasonal in nature: Fewer people donate blood during the holidays, the weather's bad, and more people are sick. This January is no different. **The nation's blood banks are asking for immediate donations to boost already critically low blood supplies. National inventory levels have dropped well**

below a safe and adequate supply. Certain critical blood types are nearing depletion and in some areas of the country elective surgeries have been postponed or cancelled, officials say. "We are joining the blood banking community to emphasize the significance of the need to donate blood," U.S. Secretary of Health and Human Services Tommy G. Thompson says. "The nation is facing critical shortages in communities across the country. If blood supplies do not immediately increase, patients, accident victims, and those whose lives depend on regular transfusions, are at risk for not getting the blood they need." About eight million volunteers donate blood each year in the United States. On any given day, about 38,000 units of red blood cells are needed for accident victims, heart surgery patients, those undergoing organ transplants, and people getting cancer treatments.

Source: http://www.ajc.com/health/content/shared-auto/healthnews/blo_o/516627.html

[\[Return to top\]](#)

Government Sector

24. *January 12, Government Executive Magazine* — **Homeland Security looks to industry to secure nation's infrastructure.** Homeland Security Department officials said Monday, January 12, that the government does not plan to place many security requirements on private industry when it comes to protecting the nation's critical infrastructure. **James Loy, the department's deputy secretary, said the federal government will back away from issuing new security mandates to industry, and instead let private companies take the lead "in most cases" to protect critical infrastructure, such as power plants and water reservoirs.** "We cannot secure the homeland from Washington, DC," Loy told a gathering of industry representatives during a conference sponsored by the department's information analysis and infrastructure protection directorate. Loy said up to 85 percent of the nation's critical infrastructure is owned and operated by private firms. Loy said the directorate's mission is to analyze potential threats against the United States, map the nation's critical infrastructure, identify ways to reduce vulnerabilities and provide industry with information. During a panel discussion before Loy spoke, Frank Libutti, DHS undersecretary for information analysis and infrastructure protection, said the department wants to partner with, rather than regulate, industry. He said private companies, however, might have to invest in better security measures.

Source: <http://www.govexec.com/dailyfed/0104/011204c1.htm>

[\[Return to top\]](#)

Emergency Services Sector

25. *January 12, Herald Sun (Australia)* — **State services on red terror alert.** Victoria will play a vital role in Australia's ambitious counter-terrorism exercise. **The nation is preparing for a multi-million-dollar drill on how to deal with chemical attacks. Federal Attorney-General Philip Ruddock yesterday said the joint federal and state exercise, known as Mercury 04, would begin in March.** Ruddock said the plans, involving several federal and state law-enforcement and emergency bodies, were unmatched in scope. "This is the first time that the chemical radiological and biological equipment that we've purchased will be tested in scenarios of potential threats," he said. The event will be staged across three states

and the Northern Territory (NT). Tasmania and the NT would be the key staging grounds, with Victoria and NSW also playing important roles. The exercises would prepare Australia to react quickly to a chemical, biological or radiological threat, Ruddock said. "One of the concerns we have is that the people who are having to respond to particular emergencies are sufficiently practiced in the skills they are going to need."

Source: http://www.heraldsun.news.com.au/common/story_page/0,5478,8366815%5E2862,00.html

[\[Return to top\]](#)

Information and Telecommunications Sector

26. *January 13, Microsoft* — **Microsoft Security Bulletin MS04–003: Buffer Overrun in MDAC Function Could Allow Code Execution (832483).** Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. **Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially–crafted packet that could cause a buffer overflow. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request.** For an attack to be successful an attacker would have to simulate a SQL server that is on the same IP subnet as the target system. A target system must initiate such a broadcast request to be vulnerable to an attack. An attacker would have no way of launching this first step but would have to wait for anyone to enumerate computers that are running SQL Server on the same subnet. Also, a system is not vulnerable by having these SQL management tools installed. Code executed on the client system would only run under the privileges of the client program that made the broadcast request. Microsoft has assigned a severity rating of "Important" to this issue.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04–003.asp>

27. *January 13, Microsoft* — **Microsoft Security Bulletin MS04–001: Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Can Allow Remote Code Execution.** A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. **An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system.** The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode. ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default. Users can prevent the risk of attack by disabling the H.323 filter. Microsoft has assigned a severity rating of "Critical" to this issue.

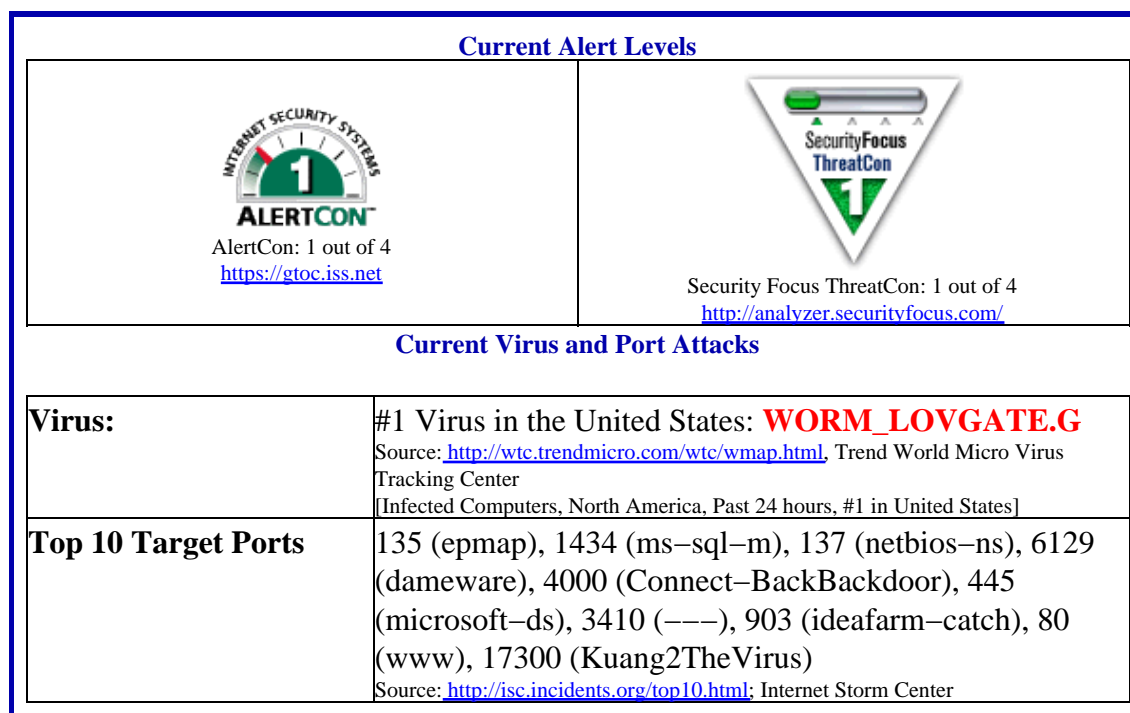
Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04–001.asp>

28. *January 13, Microsoft* — **Microsoft Security Bulletin MS04-002: Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation.** A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing Outlook Web Access (OWA) and, OWA on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front-end server and OWA might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. **The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA.** This vulnerability is exposed if the Website that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. Microsoft has assigned a severity rating of "Moderate" to this issue.
Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-002.asp>
29. *January 12, esecurityplanet.com* — **Buffer overflow plugged in Sun ONE web server. Sun Microsystems on Monday, January 12, warned of a buffer overflow vulnerability in its Sun ONE/iPlanet Web Server product.** The firm said the **flaw could be exploited by a remote user to crash the Web server, which is a type of denial-of-service attack.** Independent research firm Secunia has rated the security hole as "moderately critical." **The vulnerability affects the Sun ONE/iPlanet Web Server 6.0 Service Pack 5 and earlier versions on the HP-UX platform. Sun has issued a new service pack to fix the flaw, noting that there are no workarounds.** The susceptible products are a crucial part of Sun's Web services initiative which falls under Sun Open Net Environment (Sun ONE) brand. The Sun ONE brand includes the Sun ONE Web Server, Sun ONE Portal Server, Sun ONE Application Server, Sun ONE Directory Server, Sun ONE Identity Server, Sun ONE Messaging Server and the Sun ONE Integration Server (all formerly iPlanet products). A service pack is available online: <http://www.sun.com/software/download/products/3f186391.html>
Source: <http://www.esecurityplanet.com/prodser/article.php/3298031>
30. *January 12, Government Computer News* — **Intelligence community seeks protection from inside threats. A team of companies is building a tool to help the intelligence community keep tabs behind its firewalls. The Voltaire system will integrate existing technology to identify suspicious activity by insiders with legitimate access to sensitive information. Voltaire is intended to make it easier for agencies to share sensitive and classified information by providing a tool to enforce access policy and prevent misuse.** The goal of Voltaire is to detect and stop the kind of activity that FBI turncoat Robert Hanssen got away with for years. Hanssen gathered and sold information about FBI counterintelligence activities by browsing through computer files to which he had access. Although he had no legitimate need to see much of the information, investigators found he was able to access it over a period of years without raising any flags. **A demonstration version of Voltaire is expected to be ready for testing by summer. Feedback from intelligence agencies will then be**

implemented into a final product.

Source: http://www.gcn.com/vol1_no1/daily-updates/24622-1.html

Internet Alert Dashboard



[\[Return to top\]](#)

General Sector

31. *January 13, Voice of America* — **Bomb explosion at mosque in Bangladesh.** In Bangladesh, security has been tightened at a well-known Muslim shrine after a bomb explosion killed three people and injured more than 30 others. Soldiers and police surrounded a 700-year-old Muslim shrine in Bangladesh's northeastern city of Sylhet Tuesday, one day after a blast killed or injured dozens of worshippers. **Police say the bomb exploded Monday night when the Hazrat Shah-Jalal shrine was packed with several thousand people.** It is the second time that a Muslim shrine has been targeted in Bangladesh in the past year. A year ago, seven people were killed when a bomb was hurled at a shrine in northwestern Tangail district. **Police are questioning more than 20 suspects including several women in connection with the blast.** More than 70 people have died in explosions in Bangladesh in recent years. In the worst incident, 17 people were killed when bombs ripped through two cinema halls in the northern town of Mymensingh in December 2002.

Source: <http://www.voanews.com/article.cfm?objectID=0F3494B6-0001-4DB1-837EF04E154FEEE7>

32. *January 13, CNN* — **National Mall security lax on 9/11 anniversary according to report.** On the second anniversary of the September 11 attacks, investigators found "persistent and severe" security deficiencies throughout the National Mall, a report concludes.

Security was supposed to have been at a heightened level in the nation's capital at the time when undercover inspections from the inspector general's office of the Department of the Interior occurred September 10 and 11. According to the office's findings, on September 10, U.S. Park Police, park rangers and contract security screeners were seen to "gather and remain in groups as opposed to dispersing individually throughout the park grounds in order to conduct more efficient surveillance and protection." "There was no sign of any patrolling or posted officers anywhere throughout the hourlong duration of this particular visit," the report said. On the following day, September 11, an assessment team revisited the mall from 1:15 to 2 p.m., according to the report. "Throughout this time, there was no visible Park Police presence," the report noted.

Source: <http://www.cnn.com/2004/US/01/13/security.report/index.html>

[\[Return to top\]](#)

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information: Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202-323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.

